TITLE: A REMOTE CONTROL SYSTEM FOR A LOCOMOTIVE HAVING USER AUTHENTICATION CAPABILITIES

FIELD OF THE INVENTION

The present invention relates generally to a remote control system for transmitting signals to a locomotive. More particularly, the present invention relates to a remote control system which can determine if a potential user of the control system is an authorized user.

BACKGROUND OF THE INVENTION

Remote control systems for controlling locomotives are known in the art. Typically, remote control systems for locomotives have two main components, namely a remote control device and a locomotive controller module. The remote control device is generally a portable unit that is carried by a human operator located at a certain distance from the locomotive. The remote control device is operative for sending command signals to the locomotive controller module. The locomotive controller module is typically mounted on board the locomotive and is adapted for receiving command signals sent by the remote control device over a wireless communication link.

When an operator would like to cause a movement of the locomotive in a certain direction, or at a certain speed, for example, he or she manipulates the controls on the remote control device in order to specify the desired parameters (i.e. forward, backwards, speed, etc...). The parameters are encoded into a command signal, which is then sent by the remote control device to the locomotive control device. The locomotive control device processes the command signal and issues local control signals to a control interface for causing the desired commands to be implemented by the locomotive.

A deficiency with existing remote control systems is that there are often no adequate security features for restricting who is able to use the remote control system for controlling a locomotive. More specifically, in many existing remote control systems, anyone can pick up the remote control device and start controlling a locomotive. For security reasons, it is not desirable for a person who is not familiar with the locomotives, or who is not authorized to use the remote control system, to be able to use the remote control device to operate the locomotive. Furthermore, in the case where an accident occurs with a locomotive, a locomotive owner is generally unable to reliably determine who was controlling the locomotive at the time of the accident.

In the context of the above, it can be seen that there is a need in the industry to provide a remote control system that alleviates, at least in part, the problems associated with the existing remote control systems.

SUMMARY OF THE INVENTION

In accordance with a first broad aspect, the present invention provides a remote control system for a locomotive. The remote control system comprises a remote control device, an identification interface and a locomotive controller module. The remote control device is operative for receiving a command signal conveying an action to be executed by the locomotive. The identification interface is located remotely from the remote control device and is adapted for receiving user identification data from a user of the remote control device. The locomotive controller module is suitable for mounting at the locomotive and is adapted for generating local control signals. When the user identification data belongs to an authorized user, the locomotive controller module is operative to issue a local control signal for causing the locomotive to execute the action conveyed by the command signal received at the remote control device.

In accordance with another broad aspect, the present invention provides a remote control device for controlling a locomotive. The remote control device comprises a first input, a second input and a processing unit. The first input is operative for

receiving from a user a command signal indicative of a command to be executed by the locomotive. The second input is distinct from the first input and is for receiving user identification data. The processing unit is operative for transmitting the control signal indicative of a command to be executed by the locomotive when the user identification data belongs to an authorized user.

In accordance with another broad aspect, the present invention provides a remote control system for a locomotive. The remote control system comprises a remote control device, a user authentication unit and a locomotive controller module. The remote control device includes a first input for receiving an input command signal from a user indicative of a command to be executed by the locomotive. The remote control device also includes a second input distinct from the first input and which is for receiving user identification data. The user authentication unit is in communication with the remote control device and is adapted for receiving the user identification data from the remote control device and processing the user identification data to generate verification data indicative of whether the user identification data belongs to an authorized user. The locomotive controller module is suitable for mounting at the locomotive and is adapted for generating local control signals on the basis of command signals originating from the remote control device. When the verification data indicates that the user identification data belongs to an authorized user, the locomotive controller module issues a local control signal for causing the locomotive to execute the command conveyed by the command signal received at the first input of the remote control device.

In accordance with another broad aspect, the present invention provides a method for controlling a locomotive. The method comprises receiving at a first input a command signal from a user indicative of a command to be executed by the locomotive and receiving at a second input, distinct from the first input user, identification data. The method further comprises transmitting a control signal indicative of the command to be executed by the locomotive when the user identification data belongs to an authorized user.

In accordance with another broad aspect, the present invention provides a remote control device for controlling a locomotive. The remote control device comprises a first input, a second input, a user authentication unit and a processing unit. The first input is for receiving a command signal from a user indicative of a command to be executed by the locomotive and the second input is operative to receive user identification data from a machine readable storage medium. The user authentication unit is operative for processing the user identification data to generate verification data indicative of whether the user identification data belongs to an authorized user. The processing unit is operative for transmitting a control signal indicative of the command to be executed by the locomotive when the verification data indicates that the user identification data belongs to an authorized user.

In accordance with an alternative aspect of the present invention, the second input is operative to receive user identification data from a user's fingerprint, from a keypad, from a retinal scanner, or from a DNA sample.

In accordance with an another broad aspect, the present invention provides a remote control system for a locomotive. The remote control system comprises a remote control device, a user authentication unit and a locomotive controller module. The remote control device includes a first input and a second input. The first input is for receiving a command signal from a user indicative of an action to be executed by the locomotive and the second input is operative for receiving user identification data from a machine readable storage medium. The user authentication unit is in communication with the remote control device, and is adapted for receiving the user identification data from the remote control device and processing the user identification data to generate verification data indicative of whether the user identification data belongs to an authorized user. The locomotive controller module is suitable for mounting at the locomotive. The locomotive controller module is adapted for generating local control signals on the basis of command signals originating from the remote control device. When the verification data indicates that the user identification data belongs to an authorized user, the locomotive controller module is operative to issue a local control signal for causing the locomotive to execute the

action conveyed by the command signal received at the first input of the remote control device.

In accordance with another broad aspect, the present invention provides a remote control device for controlling a locomotive. The remote control device comprises a first input, a second input and a processing unit. The first input is operative for receiving a command signal from a user indicative of a command to be executed by the locomotive and the second input is operative to receive user identification data. The remote control device is operative to prompt the user to provide user identification data. The processing unit is operative to transmit a control signal indicative of a command to be executed by the locomotive when the user identification data is determined to belong to an authorized user.

In accordance with yet another broad aspect, the present invention provides a remote control system for a locomotive. The remote control system comprises a remote control device, a user authentication unit and a locomotive controller module. The remote control device includes a first input and a second input. The first input is for receiving a command signal from a user indicative of an action to be executed by the locomotive and the second input is operative for receiving user identification data. The remote control system is operative for prompting the user to input the user identification data. The user authentication unit receives the user identification data from the remote control device and processes the user identification data to generate verification data indicating whether the user identification data belongs to an authorized user. The locomotive controller module is suitable for mounting at the locomotive. The locomotive controller module is adapted for generating local control signals on the basis of command signals originating from the remote control device. When the verification data indicates that the user identification data belongs to an authorized user, the locomotive controller module issues a local control signal for causing the locomotive to execute the action conveyed by the command signal received at the first input of the remote control device.

In accordance with another broad aspect, the present invention provides a remote control device for controlling a locomotive. The remote control device comprises a first input, a second input, an authentication unit and a processing unit. The remote control device is operative for receiving a command signal from a user indicative of a command to be executed by the locomotive. The second input is operative for receiving user identification data. The authentication unit is operative for processing the user identification data to generate verification data indicative of whether the user identification data belongs to an authorized user. The processing unit is operative for transmitting a control signal indicative of a command to be executed by the locomotive when the user authentication unit confirms that the user identification data belongs to an authorized user. The processing unit is responsive to a transmission termination event to cease the transmission of control signals indicative of commands to be executed by the locomotive .

In accordance with yet another broad aspect, the present invention provides a remote control system for a locomotive. The remote control system comprises a remote control device, a user authentication unit and a locomotive controller module. The remote control device includes a first input and a second input. The first input is for receiving command signals from a user indicative of an action to be executed by the locomotive and the second input is operative for receiving user identification data. The user authentication unit receives the user identification data from the remote control device and processes the user identification data to generate verification data indicative of whether the user identification data belongs to an authorized user. The locomotive controller module is suitable for mounting at the locomotive and is operative for generating local control signals on the basis of command signals originating from the remote control device and issuing a local control signal for causing the locomotive to execute the action conveyed by the command signal received at the first input of the remote control device, when the verification data indicates that the user identification data belongs to an authorized user. In response to a transmission termination event, the locomotive controller module is adapted to cease the transmission of local control signals .

These and other aspects and features of the present invention will now become apparent to those of ordinary skill in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings:

Figure 1 shows a block diagram of a remote control system in accordance with a first specific example of implementation of the present invention;

Figure 2 shows a block diagram of a remote control system in accordance with a second specific example of implementation of the present invention;

Figure 3 shows a block diagram of a remote control system in accordance with a third specific example of implementation of the present invention;

Figure 4 shows a specific, non-limiting example of a physical embodiment of a remote control device in accordance with a non-limiting example of implementation of the present invention;

Figure 5 shows a flow chart of a process for operating the remote control system in accordance with a first specific example of implementation of the present invention;

Figure 6 shows a flow chart of process for opreating the remote control system in accordance with a second specific example of implementation of the present invention;

Figure 7 shows a flow chart of a process for operating the remote control system in accordance with a third specific example of implementation of the present invention; and

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

DETAILED DESCRIPTION

Shown in Figure 1 is a block diagram of a remote control system 10 in accordance with a first specific example of implementation of the present invention. The remote control system 10 includes a remote control device 12, a locomotive controller module 14 that is adapted for being mounted on board a locomotive 18, an identification interface 20, and a user authentication unit 22. As will be described in more detail further on in the description, the identification interface 20 is operative for receiving user identification data from a user. The received user identification data is forwarded to the user authentication unit 22, which determines if the user identification data belongs to an authorized user of the remote control system 10.

The remote control device 12 includes an input 24 for receiving command signals from a user that are indicative of commands to be executed by the locomotive 18. The command signals can convey any useful commands including but not limited to speed commands, braking commands, direction commands, throttle commands, coast commands, etc...The remote control device 12 further includes a processing unit 28 that is in communication with input 24 for receiving the command signals. The processing unit 28 transmits signals conveying the commands to be executed by the locomotive 18 to the locomotive controller module 14 over a wireless communication link 26.

In a specific embodiment of the present invention, the remote control device 12 is a portable unit that can be carried by an operator located remotely from the locomotive 18. However, in an alternative embodiment, the remote control device 12 is a fixed device that is mounted at a remote location from the locomotive 18, such as in a control tower or in an operator station.

As mentioned above, the locomotive controller module 14 is suitable for being mounted at a locomotive 18. The locomotive controller module 14 includes an input 30 for receiving the signals sent from the remote control device 12 over the wireless

communication link 26. The locomotive controller module 14 further includes a processing module 32 for generating local control signals on the basis of the signals sent from the remote control device 12. As will be described in more detail further on in the description, when the user identification data entered at the identification interface 20 belongs to an authorized user of the remote control system 10, the processing module 32 is able to issue the local control signals to a control interface 34 for causing the locomotive to execute the commands conveyed by the signal sent by the remote control device 12.

For the purposes of the present description, the term "control interface 34" refers globally to the collection of various actuators located on the train for executing various local control signals issued by the locomotive controller module 14. Examples of such actuators include the actuators that control the throttle and the brakes, among others.

The identification interface 20 is operative for receiving user identification data entered by a user. In a specific example of implementation, the user identification data includes user-supplied information such as a code entered via a keypad or touch sensitive screen or the use of a personalised key. Alternatively, the user-supplied information can be stored on a computer readable storage medium such as, for example, a swipe card, smart card/ and PDA. In a further specific example of implementation, the user identification data includes a biometrics parameter, such as fingerprint data, retinal scan data, voice-recognition data, DNA data and body part shape or pattern data.

It should be understood that the identification interface 20 includes hardware and software that is adapted for receiving the user identification data. As such, the identification interface 20 can include a keypad, a touch-sensitive screen, an input capable of reading a computer readable storage medium, a key hole, a fingerprint reader, a retinal scan reader, a voice interface or any other suitable type of reader known in the art for receiving user identification data.

In the specific example of implementation shown in Figure 1, the identification interface 20 is in communication with the user authentication unit 22. The user authentication unit 22 is operative for receiving the user identification data and for processing the user identification data in order to generate verification data indicating whether the user identification data belongs to an authorized user of the remote control system 10.

In a specific example of implementation, the user authentication unit 22 includes a memory (not shown) for storing a database containing information associated to authorized users of the remote control system 10. As such, upon receipt of user identification data from the identification input 20, the user authentication unit 22 processes the user identification data along with the database to determine if the received user identification data matches data stored in the database that is associated to an authorized user.

For example, in the specific case where the user identification data is fingerprint information, the user authentication unit 22 includes a database that stores fingerprint information associated with authorized users of the remote control system 10. As such, upon receipt of fingerprint information from the identification interface 20, the user authentication unit 22 processes the entries in the database to determine if the received fingerprint information matches fingerprint information contained in the database. In the case where a match is found, the user authentication unit 22 generates verification data indicating that the user identification data belongs to an authorized user. However, if no match is found, the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user. The authentication unit 22 may use any suitable fingerprint matching algorithm and the present invention is not limited to the specific algorithm used for performing fingerprint matching. Such algorithms are known in the art of fingerprint processing and as such will not be described.

Similar systems may be implemented using biometric information other than fingerprint information, such as, but not limited to, voice recognition, DNA data,

retinal scan and body shape/pattern data.

Alternatively, in the specific case where the user identification data is a pass code, the user authentication unit 22 includes a database that stores a plurality of pass codes associated respective authorized users of the remote control system 10. Upon receipt of a pass code from the identification interface 20, the user authentication unit 22 processes the database to determine if the received pass code matches a pass code contained in the database. In the case where a match is found, the user authentication unit 22 generates verification data indicating that the user identification data belongs to an authorized user. However, if no match is found, the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user.

In the specific case where the user identification data is stored on a swipe card, the user identification data can include information that indicates to the user authentication unit 22 that it belongs to an authorized user. As such, on the basis of the information, the user authentication unit 22 generates validation data indicative that the swipe card belongs to an authorized user, or that the swipe card does not belong to an authorized user. However, the user authentication unit is not able to attribute the swipe card to a specific authorized user.

In an alternative embodiment where the user identification data is stored on a swipe card, the user identification data can include information that is unique to a specific user. In such a case, the user authentication unit 22 includes a database that stores information associated with authorized users of the remote control system 10. As such, upon receipt of the unique information from the swipe card, the user authentication unit 22 processes the database to determine if the information from the swipe card matches an entry contained in the database. In the case where a match is found, the user authentication unit 22 generates verification data indicative that the user identification data belongs to an authorized user. However, if no match is found, the user authentication unit 22 generates verification data indicative that the user identification data does not belong to an authorized user.

When the user identification data is unique to a specific user, such as a fingerprint, retinal data, DNA data, a unique pass code, or unique information stored on a swipe card, the user authentication unit 22 is able to determine which authorized user has entered his/her user identification information. As such, in a specific example of implementation, the user authentication unit 22 includes a memory in which it is able to keep a record of the log-in time of the authorized user. Optionally, the user authentication unit 22 is able to keep a record of the log-out time of an authorized user on the basis of transmission termination events, which will be described in more detail. Beneficially, by keeping a record of a specific user's log-on and log-off times, an administrator of the remote control system 10 is able to know who was using the remote control device 12 during a certain time period.

In a variant, in order for the user authentication unit 22 to generate validation data indicating that the user identification data belongs to an authorized user, the user authentication unit 22 may make use of a combination of information data elements from the user. For example, the user authentication unit 22 may require fingerprint information as well as a pass code from the user in order to determine if the user is an authorized user.

In the embodiment shown in Figure 1, the user authentication unit 22 is in communication with the processing unit 28 of the remote control device 12 over a communication link 36. Preferably, communication link 36 is a wireless communication link such as a radio-frequency communication link or an infrared communication link, however, it is within the scope of the present invention for communication link 36 to be a wireline communication link.

In a specific example of implementation, when the user authentication unit 22 generates verification data indicating that the user identification data belongs to an authorized user, the user authentication unit 22 transmits a verification signal to the remote control device 12 over communication link 36. Upon receipt of that verification signal, the processing unit 28 transmits the commands conveyed by the

signals received at input 24 to the locomotive controller module 14. In this fashion, an authorized user is able to control the locomotive 18.

However, when the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user, the user authentication unit 22 does not transmit a verification signal to the processing unit 28. In the absence of the verification signal, the processing unit 28 does not transmit signals conveying the commands to the locomotive controller module 14. In an alternative embodiment, when the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user, the user authentication unit 22 transmits a verification signal indicating that the user identification data does not belong to an authorized user. In response to this verification signal the processing unit 28 does not transmit command signals to the locomotive controller module 14. In either case, an unauthorized user is unable to operate the locomotive 18.

In a variant, the authentication unit 22 is in communication with the locomotive controller module 14 over a communication link 38 (indicated by dotted lines in Figure 1) instead of communication link 36. Preferably, communication link 38 is a wireless communication link such as a radio-frequency communication link or an infrared communication link, however, it is within the scope of the present invention for communication link 38 to be a wire-line communication link. In addition, communication link 38 can be distinct from communication link 26, or alternatively, they can be the same communication link. For example, communication link 26 and communication link 38 might share the same RF frequency.

In this variant, the processing unit 28 of the remote control device 12 transmits the command signals to the locomotive controller module 14 over communication link 26 regardless of whether they are entered by an authorized user. As such, it is the processing module 32 that receives verification signals from the user authentication unit 22 indicating whether the user is an authorized user. In a specific example of implementation, when the user authentication unit 22 generates verification data

indicating that the user identification data belongs to an authorized user, the user authentication unit 22 transmits a verification signal to the processing module 32 over communication link 38. In response to the verification signal, the processing module 32 issues local control signals to the control interface 34 for causing the locomotive to execute the commands received at input 24 of the remote control device 12. As such, an authorized user is able to control the locomotive 18.

When the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user, the user authentication unit 22 does not transmit a verification signal to the processing module 32. In the absence of a verification signal, the processing module 32 does not issue local control signals to the control interface 34. In an alternative embodiment, when the user authentication unit 22 generates verification data indicating that the user identification data does not belong to an authorized user, the user authentication unit 22 transmits to the locomotive controller module 14 a verification signal indicating that the user identification data does not belong to an authorized user. In response to this verification signal, the processing module 32 does not issue local control signals to the control interface 34. As such, an unauthorized user is unable to operate the locomotive 18.

The above process will be described in more detail herein below with reference to the flow chart shown in Figure 5 and with reference to Figure 1. At step 52 a command signal conveying a command to be executed by the locomotive 18 is received at input 24 of the remote control device 12. At step 54, user identification data is received at identification interface 20. At step 56, the user authentication unit 22 processes the user identification data in order to determine if it belongs to an authorized user. At step 58, when the user authentication unit 22 determines that the user identification data belongs to an authorized user, the processing module 32 of the locomotive control device 14 is enabled to transmit local control signals to the control interface 34 for causing the locomotive to execute the commands conveyed by the signal provided at the remote control device 12. For step 58, the user authentication unit 22 can send the verification signal to the remote control device 12 or to the locomotive

controller module 14 to enable local control signals to be sent to the control interface 34.

Figure 5 shows step 52 as being performed independently of steps 54 and 56. In other words, receiving a command signal at input 24 is not necessarily dependent on receiving user identification data at the identification interface 20. It is within the scope of the invention for the remote control device 12 to receive and transmit a plurality of signals conveying commands received at input 24 over communication link 36 having only received user identification data once. For example, a user may only need to enter user identification data when he or she starts using the remote control device 12, and then doesn't need to enter user identification data again. The different scenarios in which the locomotive controller module 14 will cease transmitting local control signals to the control interface 34 will be described in more detail later on in the specification.

In an alternative example of implementation, user identification data can be entered by the user each time the user enters a command signal at input 24. As such, the user's authorisation is verified each time a command is entered at input 24.

In the specific example of implementation shown in Figure 1, the identification interface 20 and the authentication unit 22 are located remotely from the remote control device 12 and the locomotive controller module 14. For example, they may be located at a central control tower, or at a location where the remote control devices 12 are stored. As such, a user can enter his/her user identification data at the identification interface 20 when they pick up their remote control device 12 prior to entering a switchyard, or other location where they are about to use the remote control device 12.

In an alternative embodiment (not shown in the Figures), the identification interface 20 and the user authentication unit 22 are located at the locomotive 18. For example, they can both be connected to, or can be an integral part of the locomotive controller module 14.

In a second specific example of implementation of the remote control system 10 (shown in Figure 2), the identification interface 20 and the user authentication unit 22 are part of the remote control device 12. As such, input 24 for receiving a command signal from a user is a first input, and the identification interface 20 for receiving the user identification data is a second input. In a specific example of implementation, the identification interface 20 can be distinct from the input 24. For the purposes of the present description, the term "distinct" means that it is separate from the first input 24. Preferably, the identification interface is dedicated to receive user identification data. In other words in this specific implementation, the identification interface 20 is not used by a user of the remote control device 12 for entering command signals. Alternatively, the identification interface 20 is embodied in the same physical input as input 24. For example, the user might enter user identification data via a keypad that can also be used for entering speed information.

In the embodiment shown in Figure 2, the processing unit 28 of the remote control device 12 is operative for transmitting command signals to the locomotive controller module 14 when the user authentication unit 22 determines that the user identification data received at input 20 belongs to an authorized user. This method will be described in more detail with reference to the flow chart shown in Figure 6. At step 60 a command signal indicative of a command to be executed by the locomotive 18 is received at the first input 24 of the remote control device 12. At step 62, user identification data is received at the second input/identification interface 20 of the remote control device 12. At step 64, the user authentication unit 22 processes the user identification data in order to determine if it belongs to an authorized user. At step 66, when the user identification data belongs to an authorized user, the processing unit 28 transmits the command conveyed by the signal received at input 24 to the locomotive controller module 14. In such an embodiment, the processing module 32 issues local control signals to the control interface for causing the locomotive to execute the commands conveyed by the remote control device 12.

As described above it is within the scope of the invention for the remote control

device 12 to transmit a plurality of signals conveying commands received at input 24 over communication link 36 having only received user identification data at the second input 20 once. For example, a user may only need to enter user identification data when he or she starts using the remote control device 12, and then doesn't need to enter user identification data again. The different scenarios in which the remote control device 12 will cease transmitting signals to the locomotive controller module 14 will be described in more detail below.

In another specific example of implementation of the remote control system 10, the identification interface 20 and the user authentication unit 22 are located at separate locations. For example, in a non-limiting example of implementation, the identification interface 20 can be located at the remote control device 12 and the user authentication device can be located either remotely from both the remote control device 12 and the locomotive controller module 14, or as shown in Figure 3, the user authentication unit 22 can be located at the locomotive controller module 14.

In the example of implementation shown in Figure 3, the processing unit 28 of the remote control device 12 transmits both the command signal and the user identification data to the locomotive controller module 14 over wireless communication link 26. As such, the user authentication unit 22 processes the user identification data when it arrives at the locomotive control unit 14. This method will be described in more detail with reference to the flow chart shown in Figure 7. At step 70 a command signal conveying a command to be executed by the locomotive 18 is received at the first input 24 of the remote control device 12. At step 72, user identification data is received at the second input/identification interface 20 of the remote control device 12. At step 74, the processing unit 28 of the remote control device transmits both the command signal and the user identification data to the locomotive controller module 14. At step 76 the user authentication unit 22 processes the user identification data in order to determine if it belongs to an authorized user. At step 78, when the user authentication unit 22 determines that the user identification data belongs to an authorized user, the processing module 32 becomes operative for issuing local control signals to the control interface 34 for causing the locomotive 18

to execute the commands conveyed by the command signal entered at the remote control device 12.

However, when the user authentication unit 22 determines that the user identification data does not belong to an authorized user, the processing module 32 does not issue local control signals to the control interface 34. As such, an unauthorized user is unable to control the locomotive 18.

It is within the scope of the invention for the processing module 32 of the locomotive controller module 14 to issue local control signals to the control interface 34 having only received user identification data at the second input 20 once. For example, a user may only need to enter user identification data when he or she starts using the remote control device 12, and then doesn't need to enter user identification data again. The different scenarios in which the locomotive controller module 14 will cease transmitting local control signals to the control interface 34 will be described in more detail below later on in the specification.

Remote control device 12

In a specific example of implementation, the remote control device 12 is a portable remote control device 12 that is adapted for being carried by a human operator located at a certain distance from the locomotive 18. A specific, non-limiting, example of a physical layout of the remote control device 12 is shown in Figure 4. The remote control device 12 shown in Figure 4 is in the form of a portable unit that includes a housing 40 for enclosing the electronic circuitry, a battery for supplying electrical power (not shown) and a user interface 42 for enabling the user to enter command signals conveying commands to be implemented by the locomotive 18.

In the specific embodiment shown, the user interface 42 includes two dials 44a and 44b located on either side of the housing 40, that are able to be manipulated by a user in order to enter command data. Specifically, by manipulating dial 44a located on the left, the user is able to enter brake commands. The brake command information is

displayed to the user via display portion 46 shown on the front of the housing 40. By manipulating dial 44b located on the right, the user is able to enter speed commands. The speed command information is displayed to the user via display portion 48 shown on the front of the housing 40. Other commands, such as on/off, bell/horn activation and forward/reverse, can be entered via control knobs and buttons 50 located on the upper portion of the housing 40. Although a specific embodiment of a remote control device 12 has been described herein, it should be understood that the physical implementation of the remote control device 12 can vary greatly without departing from the spirit of the invention.

In the case where the identification interface 20 is included as part of the remote control device 20, as described above with respect to Figures 2 and 3, the user interface 42 of the remote control device 12 includes an input 51 for receiving the user identification data. Preferably, the input 51 is a distinct input designed for receiving user identification data. In the specific embodiment of a remote control device 12 shown in Figure 4, the input 51 is a distinct input for receiving user identification data in the form of fingerprint information.

In addition, the specific embodiment shown in Figure 4 includes a visual prompt 53, in the form of a flashing light in order to prompt the user to enter user identification data. Other types of prompts 53 such as audio prompts, text prompts or any other suitable form of prompt known in the art could also be used without departing from the spirit of the invention in order to instruct the user of the remote control unit 12 to provide user identification data.

Preferably, the prompt would be active until a user enters user identification data. The term "active" as used herein, means that the prompt indicates to the user that user identification data should be entered. For example, the prompt may flash intermittently, be lit up, display text, make a noise, or provide any other type of indication to the user. Once the user has been identified as an authorized user, the prompt would cease to be active until a termination transmission event occurs, which will be described in more detail herein below.

Transmission Termination Events

Typically, in use, an operator of the remote control system 10 provides user identification data when he or she wishes to start using the remote control device 12. As such, once the user identification data has been determined by the user authentication unit 22 to belong to an authorized user, the user is enabled to control the locomotive 18 until a transmission termination event occurs. However, in response to a transmission termination event, the remote control system 10 prevents a user from controlling the locomotive 18 until new user identification data that belongs to an authorized user is provided. For example, depending on how the remote control system 10 is configured, the transmission termination event could cause processing unit 28 of the remote control device 12 to cease transmitting signals conveying commands to the locomotive controller module 14. As such, once a transmission termination event occurs, the remote control device 12 cannot control the locomotive 18 until new user identification data that belongs to an authorized user is received at the identification interface 20. Alternatively, the transmission termination event could cause the processing module 32 to cease transmitting local control signals to the control interface 34.

In a first specific example of implementation, the transmission termination event causes a prompt signal to be provided by the user. The signal indicates to the user that the locomotive 18 cannot be controlled by a user until user identification data belonging to an authorized user is entered at the identification interface 20.

In a specific non-limiting example of implementation, the user interface 42 of the remote control device 12 includes a user input for enabling the user to enter the termination signal. As such, once the user of the remote control device 12 is finished using the remote control device 12, the user can simply activate the user input in order to enter the termination signal. Upon receipt of the termination signal, the processing unit 28 of the remote control device 12 prevents command signals from being sent to

the locomotive controller module 14 until new user identification data belonging to an authorized user is entered at the identification interface 20.

Alternatively, the user input for enabling the user to enter a termination signal could be located at the locomotive. As such, once the user of the remote control device 12 is finished using the remote control device 12, the user can simply activate the user input in order to enter the termination signal. Upon receipt of the termination signal, the processing module 32 of the locomotive controller module 14 ceases to transmit local control signals to the control interface 34 until new user identification data belonging to an authorized user is entered at the identification interface 20.

In an alternative example of implementation, the transmission termination event includes the expiration of a time delay commencing upon receipt at the identification interface 20 of a signal indicative of user identification data that belongs to an authorized user. For example, when the user authentication unit 22 determines that the user identification data entered at the identification interface 20 belongs to an authorized user, a timer is started. Upon expiration of a predetermined amount of time, a user is no longer able to control the locomotive 18 via the remote control system 10. It should be understood that the timer can be included at either the user authentication unit 22, the processing unit 28 of the remote control device 12, or the processing module 32 of the locomotive controller module 32. As such, in the case where the timer is located at the processing unit 28 of the remote control device 12, or in the case where the timer is located at the user authentication unit 22 that is in communication with the remote control device 12, upon expiration of the predetermined amount of time, the processing unit 28 ceases to transmit signals indicative of commands entered at input 24 to the locomotive controller module 14. In the case where the timer is located at the processing module 32 of the locomotive controller module 14, or in the case where the timer is located at the user authentication unit 22 that is in communication with the locomotive controller module 14, upon expiration of the predetermined amount of time, the processing module 32 ceases to transmit local control signals to the control interface 34.

The pre-determined amount of time can be a specific amount of time, such as 6 hours, which might represent the working shift of a user of the remote control device 12. As such, the user would enter his or her user identification data at the beginning of a shift and be able to control the locomotive 18 throughout the length of his or her shift. However, when the shift is over, such as after the pre-determined 6 hours, remote control system 10 would automatically stop controlling the locomotive 18 until new user identification data belonging to an authorized user is entered at the identification interface 20.

In an alternative example of implementation, the transmission termination event can include the expiration of a time delay during which no signal indicative of a command to be executed by the locomotive is received at input 24 of the remote control device 12. In such an embodiment, a timer located at the remote control device 12 would begin each time a user enters a command signal at input 24, such that each time the user enters a new command the timer is reset. Upon the expiration of a pre-determined time delay during which no command signal is received at input 24, the remote control system 10 would automatically stop controlling the locomotive 10, until new user identification data is received at the identification interface 20.

In yet another alternative example of implementation, the remote control system 10 does not receive a transmission termination event, and as such, user identification data must be entered by the user each time the user enters a command signal at input 24. As such, the user's authorisation is verified each time a command is entered.

In a further specific example of implementation, the processing unit 28 of the remote control device 12 is in communication with a memory unit suitable for storing a history of the commands entered by a specific user. For example, once the user has entered his or her user identification data the processing unit 28 is able to access a file associated to that user. The file may include data elements indicative of the user's name, the times and dates when that user was using the remote control device 12, and a list of commands entered by that user. In addition, once the user has entered his or her user identification data, the processing unit 28 is further able to add to that file all

the commands entered by the user during the time he or she uses the remote control device 12. Such a feature is advantageous for security reasons because it enables an owner, or other administrator of the remote control system 10, to determine who was operating the remote control device 12 at all times. Alternatively, the memory is with the authentication unit 22 and only stores login and logoff times.

Although the present invention has been described in considerable detail with reference to certain preferred embodiments thereof, variations and refinements are possible without departing from the spirit of the invention. Therefore, the scope of the invention should be limited only by the appended claims and their equivalents.